5 Короткі повідомлення

УДК 621.318

ВОЗМОЖНОСТИ АППАРАТНОЙ РЕАЛИЗАЦИИ ЭЛЕМЕНТОВ ДСТУ 4145-2002

Георгий Гусев
МП "ДИНА"

Анотація: **Наведено три приклади експериментальних проектів апаратної реалізації в логічних інтегральних схемах, що програмуються, деяких алгоритмічних структур, які є властивими для обчислення і перевірки цифрового підпису згідно зі стандартом ДСТУ 4145-2002.**
Summary: **It represented three examples of experimental designs for implementation in programmable logic devices of some algorithmic structures, which is typical to calculate and check of the digital signature in according to standard DSTU 4145-2002.**
Ключові слова: **Цифровий підпис, еліптична крива, логічні інтегральні схеми, що програмуються.**

Аппаратная реализация процедур, используемых при вычислении и проверке цифровой подписи вызвана стремлением решить проблему генерации и хранения секретных ключей цифровой подписи в отделяемых от компьютера специальных устройствах (картах и т. п.), а также сократить время обработки документов, снабжаемых цифровой подписью.

До появления на рынке специальных кристаллов для вычисления и проверки цифровой подписи целесообразно применение программируемых логических интегральных схем (ПЛИС). Возможность вычисления координат точек эллиптической кривой при многократном применении небольшого ряда формул в процедурах вычисления и проверки цифровой подписи создает предпосылки для создания в ПЛИС однотипных многоразрядных цифровых структур, которые используются многократно в параллельном режиме, а также могут быть использованы и последовательно во времени при поэтапных вычислениях. Например, алгоритм удвоения точки эллиптической кривой включает 4 операции возведения в степень (2, 4), 4 операции сложения, 4 операции умножения, где каждый разряд вычисляется по алгоритму, подобному другим разрядам. Эти операции типичны для процедур вычисления цифровой подписи.

Опытная разработка проектов, помещающих в ПЛИС семейства ACEX фирмы Altera алгоритм удвоения точки в поле степени $m = 173$, демонстрирует возможности реализации таких алгоритмов в кристаллах небольшого размера ($50 - 100$ тысяч вентилей). В проектах используются 173-разрядные сдвиговые регистры. Умножение двух элементов базового поля, хранящихся в сдвиговых регистрах, реализуется логическими цепочками, содержащими элементы "и" и "исключающее или" количеством, соответствующим степени базового поля и объединенными выходами через многовходовой элемент "исключающее или". С целью ускорения вычислений предусматривалось одновременное вычисление двух и четырех разрядов произведения, а также использование блоков оперативной памяти ПЛИС для хранения исходных и промежуточных данных. Моделирование вычислений в указанных проектах демонстрирует удвоение точки эллиптической кривой за 6,3 мксек и 3,2 мксек (при одновременном вычислении 4 разрядов произведения).

При подобной реализации процедуры сложения двух точек эллиптической кривой вычисление цифровой подписи оценивается за время около 0,6 мсек., что сравнимо с выполнением этой процедуры на современных компьютерах с тактовой частотой процессора 1 ГГц и более. Очевидно, что применение более крупных и быстродействующих ПЛИС позволит увеличить производительность таких систем.

При создании архитектуры вычислительных систем с многократными повторениями одинаковых операций над многоразрядными операндами с целью повышения производительности целесообразно минимизировать пересылки данных, особенно в малоразрядных и медленнодействующих интерфейсах.